Consulting with Checklists

Gregory J. Brill

Booz Allen Hamilton

Objectives

Based on Booz Allen Hamilton's extensive experience providing consulting services:

- Provide an overview of services that leverage checklists
- Discuss how checklists increase efficiency and add value to customers
- Discuss trends in client needs, including the usability and functionality of checklists
- Discuss general advantages and disadvantages of checklists
- Address the potential benefits and challenges to internal development of checklist by software developers

Services That Leverage Checklist Strategies, Range From Simple to Complex

- Development of methodologies to determine compliance with security requirements and/or policies
  - General security objectives in categories such as personnel, general computer security, policy and procedures
  - Platform-specific such as Windows, Unix, and Mainframe Security
  - Test the implementation of new security policies
- Development of self-assessment methodologies
  - Leverage checklists that are designed to provide sufficient detail to be used by a wide range of skill sets
  - Leverage a risk based approach
- Checklists are leveraged in performing Certification and Accreditations
  - Security Test and Evaluation (ST&E)
  - Lower risk systems are evaluated using a checklist approach
- Develop databases to manage checklists

Services That Leverage Checklist Strategies, Range From Simple to Complex (cont)

- Consult with vendors in developing checklists for client base for use in automated tools
  - General objectives and test procedures
  - Platform specific security configurations and settings
  - Client tailored
- Develop checklists intended for information gathering:
  - Inventorying hardware and software
  - Determining risk attributes such user base, interconnections, data types
  - Determining risk classification of systems

Checklists Improve the Efficiency and Consistency of the Assessment Process, Increasing Value to the Customer

- Checklists increase standardization and consistency by:
  - Ensuring identical objectives and tests are evaluated for each assessment
  - Reducing evaluator bias and reliance on experience
  - Collect similar information providing a means for performing trend analysis
- Checklists increase efficiency and effectiveness by:
  - Focusing objectives in high risk areas or configuration settings rather then performing detailed and extensive reviews
  - Increasing the number of systems that can be assessed, while leveraging limited resources and time constraints
- Training can be focused on specific security areas
  - Reduces time to prepare individuals in performing assessments
  - Knowledge transfer to customers is part of the role out in deploying checklist strategies, increasing customer skill base

Customer Needs Continue to Drive the Usability and Functionality of Checklists

- Self Assessments programs need to simulate on-site evaluations
  - "Push" the assessment process out
  - Fully explained settings, objectives, test procedures and risks within the checklist
  - Results need to be similar to an independent and objective review
- Checklists should be designed to be "easily" tailored to meet changing needs
  - Allow the ability to add organizational objectives
  - Address changes in federal guidance, such as FISMA
- Ensure flexibility by providing as many configuration settings as possible to select "checklist of the month"
- Customers increasingly want to see platform specific checklist
  - Operating Systems/ Security Packages (Windows, Unix, RACF, ACF2, Top Secret)
  - Databases
  - Telecommunication Devices (firewall and router configurations)
  - Business Applications

Customer Needs Continue to Drive the Usability and Functionality of Checklists (Cont)

- Increase in automated evaluation tools from trusted sources (i.e. vendors)
  - Standardized scripts/programs from vendors (less risk of adverse effects on systems then from proprietary versions)
  - Ability to monitoring configuration changes in real-time
  - Ability to collect, analyze and report using web based applications
  - Ability to assess systems on the entire network vs. just stand alone
- More robust methods of reporting results
  - Ability to establish a baseline and monitor progress
  - Trend identification across the enterprise
  - Relative measure of compliance

Advantages and Disadvantages of Checklists

- Advantages
  - Development time is relatively low (document based tools)
  - Quick and easy way to gather information and assess “health”
  - Can be designed to be used by both security and non-security experts
  - Provide a uniform approach to performing basic security reviews
  - Can be deployed to a large number of sites
  - Lower level of effort to train users
- Disadvantages
  - User acceptance is significantly reduced when checklists are too complex or have an extensive number of objectives/questions
  - Checklists often do not account for mitigating controls/or other factors
  - Lack of proper change control reduce the life span of the checklist
  - Results are still dependent on additional analysis from specialists
  - Self-assessments lack independence and often objectivity and are a challenge to deploy
  - Typically focused on the operating system, not the business application

Vendor/Software Developed Checklists

- Benefits of vendor developed checklists
  - Product developers have a deep technical knowledge of software, especially new releases
  - Checklists can be released with software; no delay in waiting for third party to review and develop
  - Product-specific, allowing for a more relevant and precise review
  - Established trust and authenticity of scripts and programs
- Challenges of vendor developed checklists
  - Checklist may be designed by software engineers vs. security specialists
  - Vendors may not be willing to expose vulnerabilities
  - Checklists may be developed with minimal knowledge of current or emerging federal needs
  - Vendors may not be fully aware of the environment where product is being used

QUESTIONS